IN THE SPECIFICATION

Please amend the specification as follows:

Please amend the paragraph on page 3, line 16 as follows:

U.S. Patent Application Serial No. [[--/---,---]] 10/302,414, entitled "METHOD AND APPARATUS FOR ENSURING RECEPTION OF CONDITIONAL ACCESS INFORMATION IN MULTI-TUNER RECEIVERS," by Peter M. Klauss, Raynold M. Kahn, Gregory J. Gagnon, and David D. Ha, attorney's docket number PD-200183, filed on November 21, 2002;

Please amend the paragraph on page 3, line 21 as follows:

U.S. Patent Application Serial No. [[--/---,---]] 10/302,416, entitled "METHOD AND APPARATUS FOR MINIMIZING CONDITIONAL ACCESS INFORMATION OVERHEAD WHILE ENSURING CONDITIONAL ACCESS INFORMATION RECEPTION IN MULTI-TUNER RECEIVERS," by Peter M. Klauss, Raynold M. Kahn, Gregory J. Gagnon, and David D. Ha, attorney's docket number PD-200184, filed on November 21, 2002;

Please amend the paragraph on page 4, line 3 as follows:

U.S. Patent Application Serial No. [[--/---,---]] 10/758,811, entitled "DISTRIBUTION OF VIDEO CONTENTUSING A TRUSTED NETWORK KEY FOR SHARING CONTENT," by Raynold M. Kahn, Gregory J. Gagnon, Christopher P. Curren and Thomas H. James, attorney's docket number PD-200290, filed on ~~same date herewith~~ January 16, 2004; and

Please amend the paragraph on page 4, line 8 as follows:

U.S. Patent Application Serial No. [[--/---,---]] 10/758,818, entitled "DISTRIBUTION OF BROADCAST CONTENT FOR REMOTE DECRYPTION AND VIEWING," by Raynold M. Kahn, Ronald Cocchi and Gregory J. Gagnon, attorney's docket number PD-200292, filed on ~~same date herewith~~ January 16, 2004.

Please amend the paragraph on page 6, line 26 as follows:

FIG. 5 is a logical flow illustrating how the host IRD and conditional access module (CAM) are operatively paired according to the preferred embodiment of the present invention;

Please amend the paragraph on page 9, line 5 as follows:

FIG. 3A is a diagram of a representative data stream 300 according to the preferred embodiment of the present invention. The first packet 302 comprises information from video channel 1 (data coming from, for example, the first program source 200A); the second packet 304 comprises computer data information that was obtained, for example from the computer data source 206; the third packet 306 comprises information from video channel 3 (from one of the third program source 200C); the fourth packet 308 includes information from video channel 1 (again, from the first program source 200A); the fifth packet 310 includes a null packet (from the NP generator 212); the sixth packet 312 includes information from audio channel 1 (again, from the first program source 200A); the seventh packet 314 includes information from video channel 1 (again, from the first program source 200A); and the eighth packet 316 includes information from [[video]] audio channel 2 (from the second program source 200B). The data stream therefore comprises a series of packets from any one of the program and/or data sources in an order determined by the controller 216. Using the SCID, the IRD 124 reassembles the packets to regenerate the program materials for each of the channels.

Please amend the paragraph on page 10, line 17 as follows:

In one embodiment, the data in the CWP, including the CW, is encrypted and decrypted via what is referred to hereinafter as an input/output (I/O) indecipherable algorithm. An I/O indecipherable algorithm is an algorithm that is applied to an input data stream to produce an output data stream. Although the input data stream uniquely determines the output data stream, the algorithm selected is such that it's characteristics cannot be deciphered from a comparison of even a large number of input and output data streams. The security of this algorithm can be further increased by adding additional functional elements which are [[non-stationary]] dynamic or non-static (that is, they change as a function of time). When such an algorithm is provided with identical input streams, the output stream provided at a given point in time may be different than the output stream provided at another time.

Please amend the paragraph on page 11, line 16 as follows:

Once the program materials have been decrypted, they are provided to the source decoder 406, which decodes the program materials according to MPEG or other standards as appropriate.

The decoded program materials may be stored in the RAM 408 or provided to devices coupled to the IRD 124 via the external interfaces 410, wherein the devices coupled to the IRD 124 can include [[or]] a media storage device 418, such as a disk drive, a presentation device 420, such as a monitor, or a networked device, such as another IRD 124.

Please amend the paragraph on page 12, line 25 as follows:

The PK is then encrypted by the service provider using the RK, to produce an encrypted PK, denoted ER(PK), wherein the ER( ) indicates that RK encryption is used and the PK indicates that the PK is encrypted. A message for the CAM 414 comprising the PK and the ER(PK) is generated by the service provider, and the message is encrypted using a conditional access message encryption algorithm to produce EM(PK, ER(PK)), wherein the EM( ) indicates that conditional access message encryption is used and the [[PK,]] ER(PK) indicates that the PK [[, ER(PK)]] is encrypted.

Please amend the paragraph on page 15, line 26 as follows:

In the portion of FIG. 7 labeled "Save to Disk or Transmit to Client IRD," the content identification (CID) information 714 is decrypted by an AES decryption algorithm (AES DECR) 716 using the RK 718 stored in the TDM 402, in order to generate a Copy Protection (CP) session key for encrypting and decrypting the program materials shared with the client IRD 124. The CID information 714 preferably comprises a content identifier that is obtained from properties and/or metadata found in the program materials, and may include copy control information (CCI).